PROBLEME DE CLASIFICARE A QUASIGRUPURILOR FINITE

Aureliu POSTORONCA,

masterand, anul II, Facultatea de Matematică și Informatică

CZU: 512.548 aurel.postoronca99@gmail.com

Teoria quasigrupurilor, în particular, a quasigrupurilor liniare se dezvoltă intens în prezent și permite soluționarea unor probleme ce țin de cifrarea și codificarea informației, combinatorică, teoria automatelor etc. [1-4]. Sistemele de criptare bazate pe quasigrupuri oferă soluții avansate pentru securizarea informațiilor. În lucrare sunt studiate proprietăți generale ale T-quasigrupurilor și clase de T-quasigrupuri cu unele condiții: identitatea medialității, identități Moufang, Bol. Sunt elaborați algoritmi pentru obținerea clasificărilor, abstracție facând de izomorfism, ale T-quasigrupurilor de ordin n≤8, peste grupul $(Z_n, +)$, cu proprietățile studiate.

Definiţia 1. Un grupoid $(Q,\cdot)$ se numeşte *quasigrup* dacă pentru orice $a, b \in Q$, ecuaţiile $a \cdot x = b$ şi $y \cdot a = b$ au câte o singură soluţie în Q.

Definiţia 2. Un quasigrup (Q, B) se numeşte *izotop* al quasigrupului (Q, A), dacă există un triplet (α, β, γ) de substituţii ale mulţimii Q, numit izotopie, astfel încât, pentru orice $x, y \in Q$, are loc egalitatea $B(x, y) = \gamma^{-1}A(\alpha x, \beta y)$. Izotopiile cu cele 3 componente egale sunt izomorfisme.

Relația de izotopie, în particular cea de izomorfism, definește o partiție pe mulțimea tuturor operațiilor de quasigrup. Problema clasificării quasigrupurilor, abstracție făcând de izotopie / izomorfism, constă în determinarea numărului acestor clase și a unor seturi de reprezentanți ai lor. Această problemă nu este soluționată integral până în prezent. În cazul grupurilor noțiunea de izotopie se reduce la cea de izomorfism: grupurile izotope sunt izomorfe [1].

Definiția 3. Un quasigrup $(Q,\cdot)$ se numește *T-quasigrup*dacă există un grup abelian $(Q, +)$, $\varphi, \psi \in Aut(Q, +)$ și un element c în Q astfel încât, pentru orice $x, y \in Q$, are loc egalitatea $x \cdot y = \varphi(x) + \psi(y) + c$.

Un quasigrup $(Q,\cdot)$ ce verifică identitatea $(x \cdot y) \cdot (u \cdot v) = (x \cdot u) \cdot (y \cdot v)$, se numește quasigrup *medial*. Conform Teoremei lui Toyoda [5], quasigrupurile mediale sunt T-quasigrupurile ce verifică condiția $\varphi\psi = \psi\varphi$. În lucrare sunt demonstrate afirmațiile prezentate în Propozițiile 1 și 2.

Propoziția 1. *Un quasigrup medial* $(Q,\circ)$*, unde* $x \circ y = \varphi(x) + \psi(y) + c$*, verifică identitatea Moufang la stânga* $x \circ (y \circ (x \circ z)) = ((x \circ y) \circ x) \circ z$ *dacă și numai dacă* $\varphi = \psi = \varepsilon$.

Corolar. *Quasigrupurile mediale cu identitatea Moufang la stânga, sunt grupuri abeliene.*

Propoziția 2. *Un quasigrup medial* $(Q,\circ)$*, unde* $x \circ y = \varphi(x) + \psi(y) + c$*, verifică identitatea Bol la stânga* $x \circ (y \circ (x \circ z)) = (x \circ (y \circ x)) \circ z$ *dacă și numai dacă* $\varphi = \psi^2 = \varepsilon$.

A fost obținută clasificarea, abstracție făcând de izomorfism, a următoarelor structuri algebrice: 1) T – quasigrupurile definite peste grupul $(\mathbb{Z}_n, +)$ al claselor de resturi modulo n, unde $n \leq 8$; 2) quasigrupurile mediale de ordinul $n \leq 8$, care verifică: a) identitatea Moufang (la stânga), b) identitatea Bol la stânga. În acest scop au fost elaborați algoritmi (și programele respective în Python) de generare a pătratelor latine de ordinul n, de clasificare a pătratelor latine, abstracție făcând de izomorfism, de generare a T-quasigrupurilor binare și verificare a unor condiții în ele. Rezultatele obținute sunt prezentate în Tabelul 1.

Tabelul 1.

Ordin	**T-quasigrupuri total peste $\mathbb{Z}_n$**	**Clase de T-quas. neizomorfe între ele, peste $\mathbb{Z}_n$**	**Quasigrupuri mediale total peste $\mathbb{Z}_n$**	**Quasigrupuri mediale Moufang peste $\mathbb{Z}_n$**	**Clase de quas. mediale Moufang neizomorfe între ele, peste $\mathbb{Z}_n$**	**Quasigrupuri mediale Bol st. peste $\mathbb{Z}_n$**	**Clase de quas. mediale Bol st. neizomorfe între ele, peste $\mathbb{Z}_n$**
2	2	1	2	2	1	2	1
3	12	4	12	3	1	6	2
4	16	4	16	4	1	8	2
5	80	8	80	5	1	10	2
6	24	4	24	6	1	12	2
7			252	7	1	14	2
8			128	8	1		

Referințe:

1. BELOUSOV, V. *Fundamentele teoriei quasigrupurilor și a buclelor*. Moscova, Nauka, 1967, 224 p.
2. DENES, J., KEEDWELL, A.D. Latin squares and their applications: Second edition. Elsevier, 2015, 440 p.
3. SIRBU, P. *Teoria quasigrupurilor. Introducere.* CEP USM, 2014, 172 p.
4. PFLUGFELDER, H.O. Quasigroups and loops: Introduction. Heldermann, Berlin, 1990.

Recomandat

***Parascovia SÎRBU**, dr., conf. univ.*